- Provide a detailed plan of your firm's proposed approach (including major tasks and sub-tasks).

AT&T Response:

Upon award, AT&T will designate project and technical leads to plan and prepare for the deployment of the WAN and VoIP. Initially, these leads will review the existing architecture, produce an integrated plan and secure project resources for project kick-off and engineering meetings.

During the project preparation phase, AT&T will produce the following:

- Integrated project schedule
- Technical architecture including all on-site and network components
- Work breakdown structure
- Project team communication plan
- Procurement plan
- Risk management plan
- Test and acceptance plan
- Operational support transition plan
- Business operations plan
- Site audit plans where required

On-Site Installation

AT&T will provide the necessary remote field deployment services to perform the equipment installation, configuration and testing. The on-site teams will be supported during the installation by a centrally-located project technical team.

For each site, AT&T will:

- Identify required changes to the router configurations.
  - The assigned Engineer is responsible for documenting all final configurations including updated floor plan.
  - All final documentation will be delivered back to the Implementation Coordinator and Project Manager.

- Coordinate on-site installation
  - Conduct Site Readiness Verification
    - Power is in place with proper receptacles
    - Circuits are in place, extended and tested
    - Rack Space is available for data network deployment
    - Cabling is completed, tested and available for use (riser and horizontal distribution)
    - Environmental needs have been accomplished
    - Construction is completed, if necessary
- Conduct site remediation via the change control process to bring site to meet system architecture standard
  - Provide the router and equipment as required.
  - Perform the cabling as required to achieve the target architecture
  - Documentation Verification
    - Scope of Work is reviewed by Project and Engineering
    - Bill of Material (i.e. router, modem)
- Scheduling
  - AT&T work orders are created to engage remote resource and dispatch technicians to the site
- On Site Installation
  - Inventory of site project equipment
    - Verify all equipment is present
    - Field Operations personnel will notify the Implementation Coordinator immediately if any equipment is missing which will impact the installation due date.
  - Perform cabling as required to achieve the target architecture
  - Rack / Stack
    - All equipment to be placed in accordance with the Rack Elevation Guide
    - Complete all physical connections
  - All equipment module/slot placement & software versions/configurations to be verified against the project documentation
    - Verify configurations on routers, switches, modems and telephones (where applicable).
  - Test and Turn-Up
    - Validate WAN and local service connectivity
    - Customer site testing will include Internet connectivity, application specific and video if applicable

  - Back up site using Site Backup guide.
  - Notify the Support Service Centers that the site is ready for site acceptance testing
- Certify site with the AT&T Support Centers
  - Update site specific Technical Network Drawings
  - Establish and test remote connectivity and operational support processes

Customer acceptance of site transformation.

- Address the functional requirements of this solicitation.

AT&T Response:

A. Technical Requirements for Managed Internet Access

Managed Internet Access as defined in the ESL as "On Premise Equipment"

Each vendor should include their Service Level Agreement (SLA) and detailed description of the terms. The SLA must address the following issues and meet the following criteria, at a minimum:

1. Network availability - industry standard of 99.999% is preferred. Service providers shall describe how they calculate availability.

AT&T Response:

This response addresses 3. "Functional Requirements", Section A. "Technical Requirements for Managed Internet Access", Tab I.b., and Tab I.d.

AT&T proposes the NetTN Wide-Area-Network to be utilized as the infrastructure for Sweetwater City Schools Managed Internet Access solution. NetTN is based on a private core network, built to meet the communication requirements for any qualifying public entity within the State of Tennessee. This infrastructure is the basis for all future services over the Internet and collaborative computing initiatives for the next several years within the State of Tennessee. The infrastructure is the enabler for building an application-aware network to link locations and efficiently transmit applications such as voice, data, and video over a single connection. Access options to connect to the network include Dedicated Private Line, Ethernet, Wireless, and xDSL (where available).

The paramount features of the NetTN network effort are security, availability and reliability. The physical NetTN core backbone network is designed to eliminate a single point of failure from isolating key network points, and minimize increases in network latency in failure scenarios. All main core backbone links between the key points are 10 Gigabit Ethernet circuits. The design has been arranged so that a failed core link will not result in excessive latency across a surviving core link. The NetTN Core backbone is scalable to 40 Gigabit services, and as end site bandwidth is ordered and aggregated, will be managed to the applicable SLAs.

AT&T, in conjunction with the Independent Local Exchange Companies, cable providers and Electric Co-op's, provides the technologies from a last mile perspective listed under the NetTN products and services page. The service offerings incorporate a universal pricing structure across the state to ensure that rural areas may participate fully in the development of electronic government services, extended education presence and information access.

NetTN NETWORK DETAILS

NetTN is a fully meshed network in compliance with the latest convergence technology. It can be scaled to any office's size and needs, and it accommodates various access methods such as DSL, Private Line, Metro Ethernet and Wavelength services. The basic design of the NetTN MPLS network allows each customer's data traffic to travel a Virtual Private Network (VPN) path from the point of entry into the network to the final destination. Customers can control which of their offices are allowed to communicate with other customer offices and those that must maintain complete separation. MPLS allows for the co-existence of all government, education, 911 and non-profit organizations on the network, along with providing the products and services needed to support new technologies and multiple options for connectivity, performance, and quality of service. The NetTN network is designed and constructed to accommodate data, voice (VoIP), multimedia and video over the same access circuit. Differentiated Services (DiffServ) is utilized within the network for end to end IP QoS features.

Network Availability

Core Backbone Availability

The Core Backbone network infrastructure of the NetTN WAN shall have a minimum monthly network availability factor of 99.999%.

Scheduled Downtime: AT&T will have no greater than 4 hours of scheduled downtime for the entire Core Backbone network infrastructure and each end site connected to the NetTN network infrastructure per quarter or 3 month period. Scheduled downtime is coordinated with the NetTN Program Office with at least 14 days advance notice prior to performing the scheduled downtime in order for the downtime not to be calculated into the monthly network availability factor.

NetTN Internet Access WAN Service Availability

Each NetTN Internet Access WAN Service Availability shall be => 99.999% per 24 hour day per calendar month. NetTN Internet Access WAN Availability will be based on a 5 minute sampling rate, presented on a per hour basis for a 24 hour day and calculated

based on the ratio of total circuit up-time over total possible circuit up-time for that 24 hour day basis for the entire calendar month.

2. Packet latency (20ms)

AT&T Response:

The NetTN Edge Device to the 1st Hop Average Round-Trip Response Time Delay shall be =<20 ms per 24 hour day per calendar month. A reading will be taken every 5 minutes, 12 samples per hour, and 288 per 24 hours. The 288 samples minus any 5 minute samples where the average bandwidth utilization is >= 80% will then be averaged together for the daily measurement.

3. Packet loss (0.5%)

AT&T Response:

Packet loss (.5%) - The NetTN Edge Device Eroded Packets shall be =< .75% total error packets (e.g., bad packets) per 24 hour day for the entire calendar month.

4. Timely installation intervals for new service requests – provide standard installation intervals for all services in the RFP

AT&T Response:

Installation intervals for new service requests vary depending on service offering. Assuming adequate facilities are available inclusive of site readiness requirements (conduit, power, etc.) the installation interval from receipt of an order to completion is 75-95 days. AT&T understands the importance of implementing services to coincide with the commencement of the e-rate funding year starting July 1st. AT&T will partner with the client to develop an implementation/project plan to meet the required service delivery intervals.

5. Maintenance response times for major and minor service outages – provide response times for major and minor outages for each service in the RFP

AT&T Response:

AT&T NetTN has three severity levels: Critical = Severity 1, Major = Severity 2 and Minor = Severity 3. The following are the response/restore times: Major problem

Identification shall result in an immediate Severity 2 ticket work log generated within 30 minutes with subsequent entries into log within two hours. Major problems shall be resolved in six hours or less. Minor problem Identification shall result in immediate Level 2 ticket work log generated within 30 minutes and subsequent entries into log within four hours. Minor Problems shall be resolved within eight hours or less.

6. Number of major failures per year

AT&T Response:

AT&T Response: AT&T's NetTN Core Network is fully redundant and is designed to minimize fiber cuts, leading to failures, if any. NetTN has Ingress/Egress to two different Internet Service Providers in two different NAPs with automatic failover. All Core Network locations (NAPs or Points of Presence [POPs]) have fiber circuit diversity, diverse fiber sheaths and fiber routes for active redundancy to other Core Network locations with the same bandwidth availability to ensure reliability of the Network. As a result, potential failures are mitigated.

7. Catastrophic incident response times (unplanned outages due to natural and man-made causes – provide response times to develop and submit a proposed resolution plan to address catastrophic outages such as hurricane, act or terror, etc.)

AT&T Response:

In the event of a catastrophic occurrence, Man-Made or Natural Disaster, AT&T will respond to customer within 4 hours post event to provide an assessment of the AT&T Network and outline service restoration efforts as required. Dedicated Service Management Team will take the lead in providing timely information to our customers, and can also assist with developing and deploying of alternative services if required.

All AT&T NetTn circuits are designated with TSP(Telecommunications Service Priority) codes to ensure high priority treatment in the restoration efforts caused by catastrophic events. Telecommunications Service Priority (TSP) is a program that authorizes national security and emergency preparedness (NS/EP) organizations to receive priority treatment for vital voice and data circuits or other telecommunications services. As a result of hurricanes, floods, earthquakes, and other natural or man-made disasters, telecommunications service vendors frequently experience a surge in requests for new services and requirements to restore existing services. The TSP Program provides service vendors a Federal Communications Commission (FCC) mandate to prioritize requests by identifying those services critical to NS/EP. A TSP assignment ensures that it will receive priority attention by the service vendor before any non-TSP service.

8. Quality of service (QoS) – voice over IP quality must be maintained at a Mean Opinion Score of 4.0, the equivalent of —toll quality.

AT&T Response:

AT&T uses the R-Factor ITU-T Recommendation as a service level objective in determining Voice over IP call quality.

Rating Factor (R-Factor) and Mean Opinion Score (MOS) are two commonly-used measurements of overall VoIP call quality.

- **R-Factor**: A value derived from metrics such as latency, jitter, and packet loss per *ITU◄T Recommendation G.107*, the R-Factor value helps you quickly assess the quality-of-experience for VoIP calls on your network. Typical scores range from 50 (bad) to 90 (excellent).
- **MOS**: A value are derived from the R-Factor per *ITU◄T Recommendation G.10* which measures VoIP call quality. PacketWise measures MOS using a scale of 10-50. To convert to a standard MOS score (which uses a scale of 1-5), divide the PacketWise MOS value by 10.

R-Factor	MOS	User Experience
90	43 (4.3)	Excellent
80	40 (4.0)	Good
70	36 (3.6)	Fair
60	31 (3.1)	Poor
50	26 (2.6)	Bad

The SLA will include consequences for noncompliance with SLAs terms, including financial penalties and grounds for contract termination (amount to be negotiated).

AT&T Response:

Each NetTN Internet Access WAN Service Availability shall be => 99.999% per 24 hour day per calendar month. NetTN Internet Access WAN Availability will be based on a 5 minute sampling rate, presented on a per hour basis for a 24 hour day and calculated

based on the ratio of total circuit up-time over total possible circuit up-time for that 24 hour day basis for the entire calendar month.

Conformance: The above NetTN Internet Access availability factor shall be calculated at the end of each calendar month and will be substantiated through performance reports generated by the NetTN Contractor.

Compensation for a Given Month: Should non-conformance apply to a given month, 1% of the total aggregate monthly costs for all affected WAN services purchased under this contract shall be paid.

Compensation for a 2nd Consecutive Month: Should non-conformance apply to a second consecutive month, 2% of the total aggregate monthly costs for all affected WAN services purchased under this contract shall be paid.

Compensation for an Nth Consecutive Month: For each consecutive month of nonconformance, **N**% of the total aggregate monthly costs for all affected WAN services purchased under this contract shall be paid, where **N** is the number of consecutive months of non-conformance.

The above compensation shall be made by the Contractor within 15 business days after each monthly NetTN Internet Access Availability report is reviewed and verified by both the TNII Association and the NetTN Contractor. The review and verification process shall be mutually scheduled between the TNII Association and NetTN Contractor for each month no greater than three weeks after the preceding month's last day.

Vendor's must provide audited financial statements for the past 3 years.

AT&T Response:

Response and documentation provided in for financial statements provided in Tab II, "Experience and Qualifications".

Vendor's must provide a detailed description of their online tools available to the client to support telecommunications payments, account information, account changes, network monitoring and other functionality that can provide value.

AT&T Response:

AT&T solutions use 2 reporting Tools - Vital Net and Business Direct

Vital Net

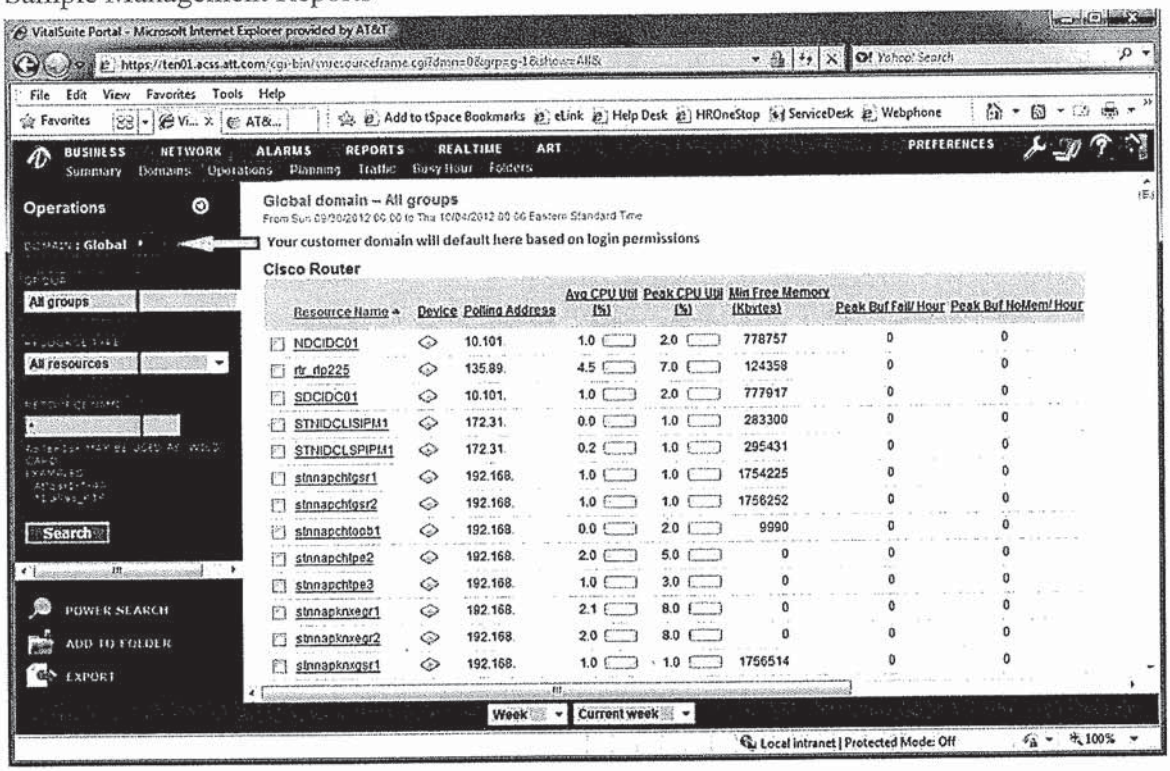
Performance and capacity management involves understanding and managing your organization's needs for network resources—most commonly involving utilization trends over time

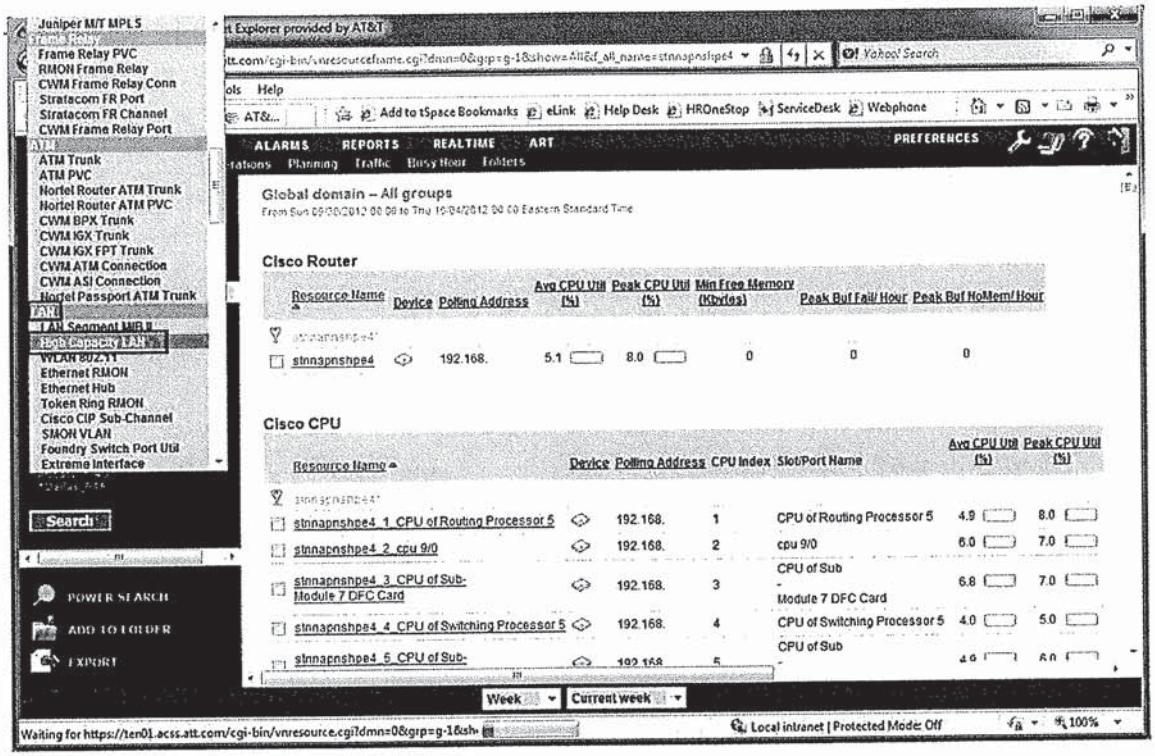
- In order to properly plan to handle the load that the community of users places on the network, one must first understand existing trends of use
- Baselines will vary depending on the patterns of use for different types of businesses

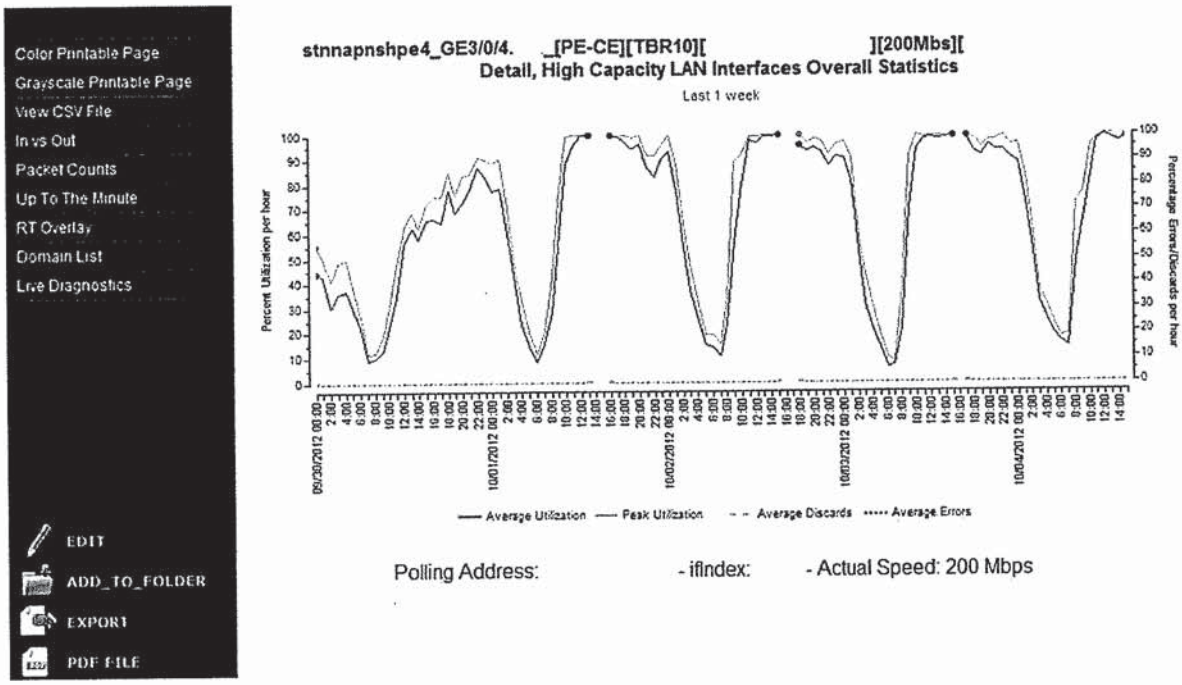
Standard Reports:

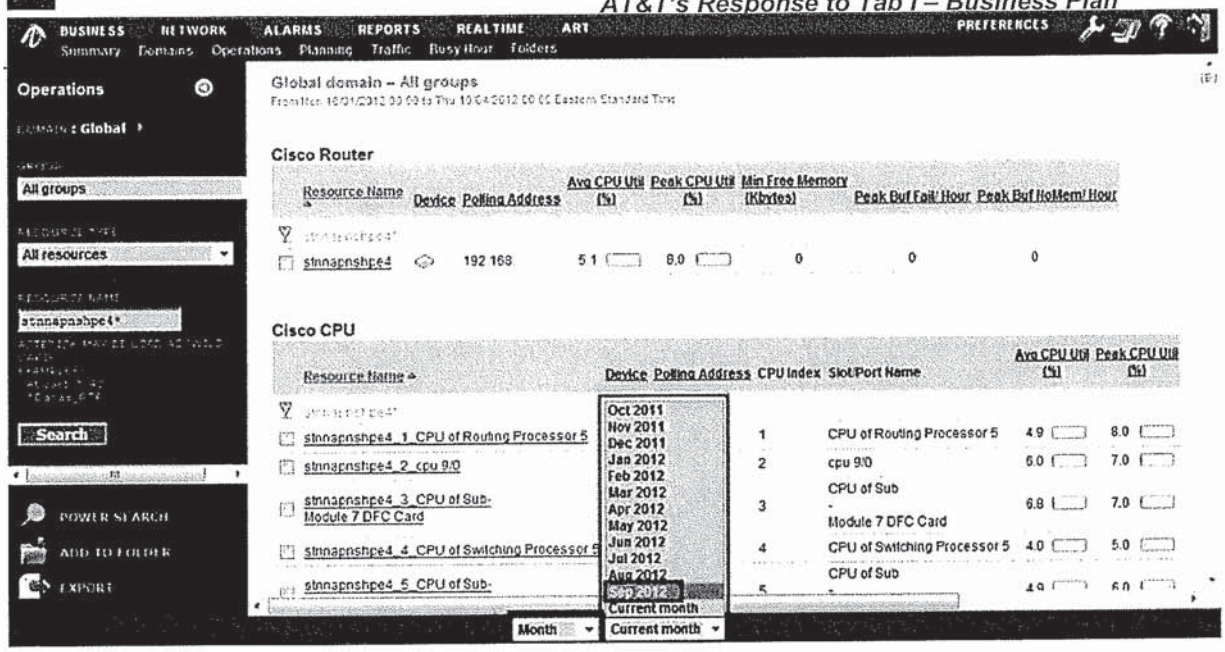
1. Summary
    - Total Network Volume
    - Average Network Volume
    - Average Health Index
    - Top 10 Situations to Watch
2. Element Detail
    - Element Volume vs. Baseline
    - Bandwidth Utilization
    - CPU Utilization (Router Report only)
3. Reports can be generated by doing drill-down to the element.
4. Reports can be customized and generated via the Web interface by using Run-A-Trend Report, Run-an-At-A-Glance Report, etc. under Organization Tab.

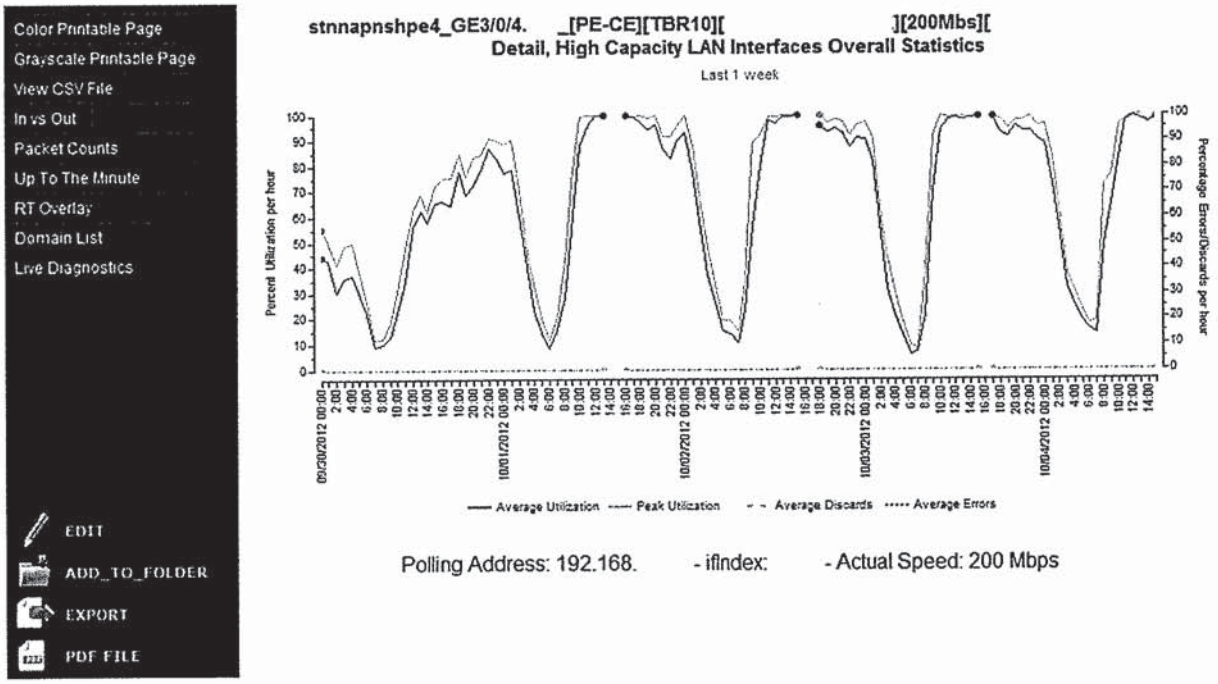
Sample Management Reports







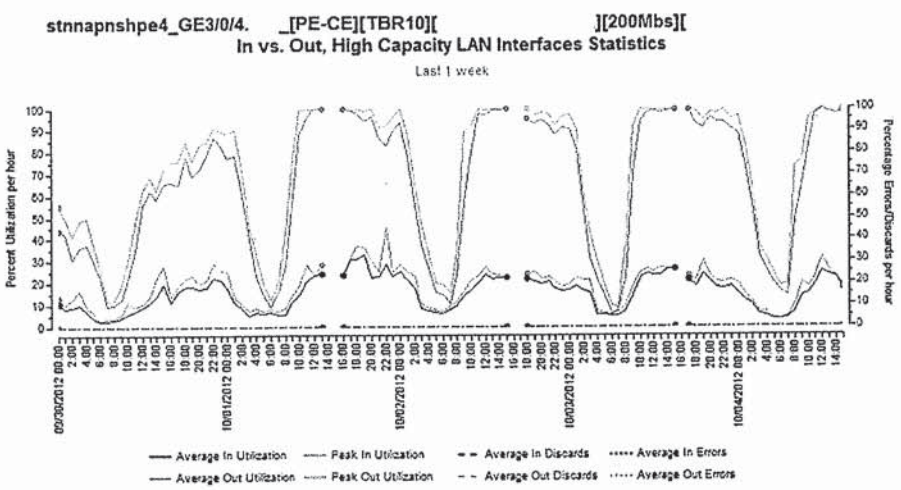




Polling Address: 192.168. - ifIndex: - Actual Speed: 200 Mbps

Color Printable Page
Grayscale Printable Page
View CSV File
Overall
Packet Counts
Up To The Minute
RT Overlay
Domain List
Live Diagnostics

EDIT
ADD_TO_FOLDER
EXPORT
PDF FILE



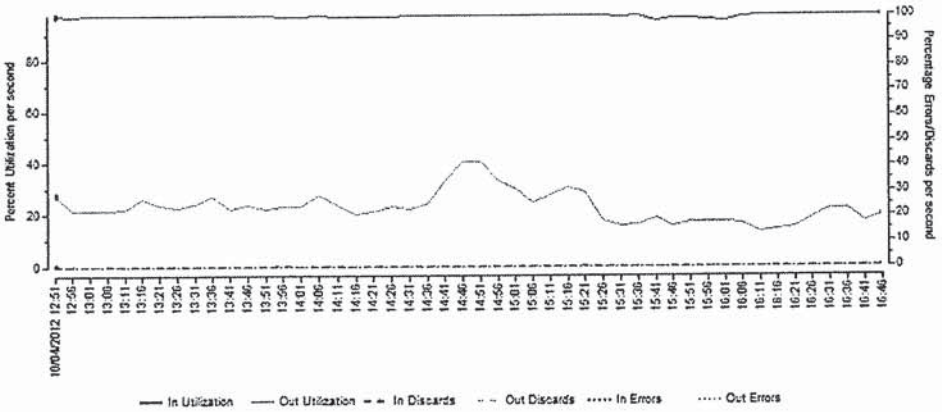
Polling Address: 192.168. - ifIndex: - Actual Speed: 200 Mbps

Color Printable Page
Grayscale Printable Page
View CSV File
Domain List
Live Diagnostics

EDIT
EXPORT
PDF FILE

STTNTBR _GE0/1_<<< To PERTR: NSHPE4 - Int Gi3/0/4
Up to the Minute, In vs. Out, High Capacity LAN Interfaces Statistics

Last 4 hours



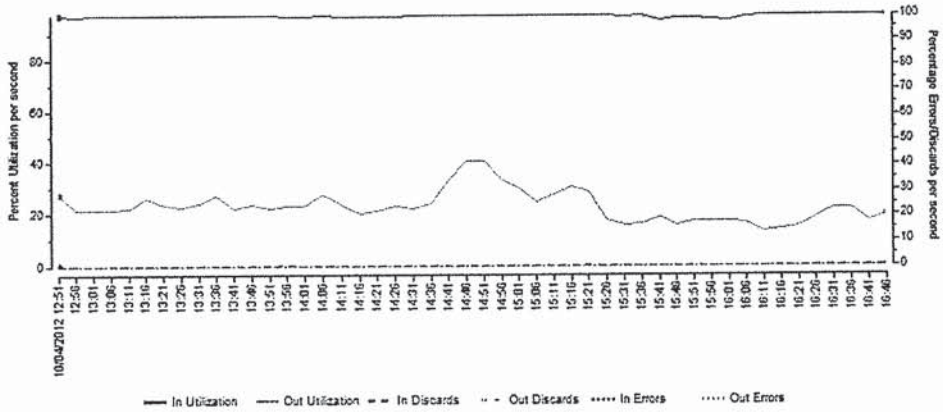
Polling Address: 172.26. - ifIndex: - Actual Speed: 200 Mbps

Color Printable Page
Grayscale Printable Page
View CSV File
Domain List
Live Diagnostics

EDIT
EXPORT
PDF FILE

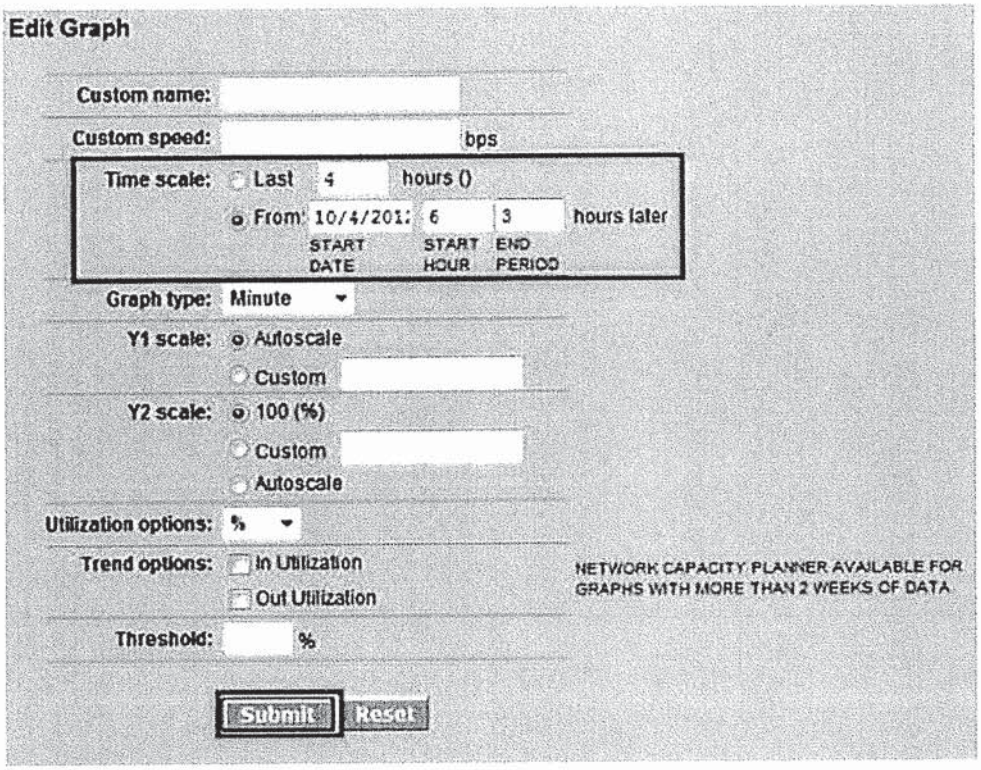
STTNTBR _GE0/1_<<< To PERTR: NSHPE4 - Int Gi3/0/4
Up to the Minute, In vs. Out, High Capacity LAN Interfaces Statistics

Last 4 hours



Polling Address: 172.26. - ifIndex: - Actual Speed: 200 Mbps

Data for any timeframe during the previous 10 days can be viewed in 5-minute granularity.



Business Direct

AT&T BusinessDirect is a suite of powerful, productivity-enhancing online tools that you can use 24 hours-a-day, 7 days-a-week to reroute network traffic in real-time, test circuits, report service problems and track them through resolution, place orders and check their status, pay bills electronically, and perform other customer service-related tasks online. AT&T BusinessDirect also includes numerous performance-reporting tools that allow customers to monitor their networks and their AT&T Managed Services, such as Website Hosting, in real-time.

The tools found on AT&T BusinessDirect are grouped into the following areas:

Ordering and Status

Through online ordering, you can have your orders filled more quickly by eliminating numerous manual steps (submit, confirm, follow up) in a typical order process, while improving order accuracy. And, you can track the progress of each order online through completion. The key ordering tool is **AT&T eOrder**.

Trouble Ticketing

AT&T BusinessDirect provides you with the capability to report service troubles online, and monitor the progress of service restoration through resolution. With AT&T BusinessDirect, you can create trouble tickets, launch circuit tests, search your listing of prior and current trouble tickets, display tickets and view their status, and communicate through a ticket log with the AT&T associate working the ticket. The key trouble ticketing tool is **AT&T eMaintenance**.

Account and Billing

The online bill viewing, analyzing, and paying capabilities help you to access your billing information quickly and easily, understand trends and charges, pay bills conveniently (and automatically if you wish), and eliminate calls to your support team. You can also question specific charges online, and they will be subtracted from your current balance due while AT&T researches your issue. The key account and billing tool is **AT&T eBill**.

Performance Reporting

AT&T's online network monitoring capabilities enable you to evaluate your network's performance and your toll-free traffic so that you can generate action plans and perform proactive planning.

AT&T BusinessDirect Map

A key performance reporting tool is **AT&T BusinessDirect Map**, which depicts your network, either U.S.-based or international, on a geographical map, lists your inventory of services, and provides the status of your service orders, trouble tickets, and network traffic levels at a glance. Numerous clickable elements enable you to drill-down for more detail.

Additional Features

AT&T BusinessDirect also includes the following features:

- **Extensive online site support.** Here you can find tutorials and archived virtual seminars, videos, FAQs, a technical glossary, and traditional help functions, all designed to facilitate your use of the portal.
- **Industry-standard security.** Site security includes Secure Sockets Layer (SSL) encryption, validation of every transaction, servers housed in state-of-the-art data centers, and a mirror-image production site for disaster recovery.
- **Alerts.** These are occasional, important, non-promotional messages from AT&T alerting you of planned maintenance activities, for example.
- **A consistent look and feel.** A consistency throughout the site provides maximum ease and usability.
-

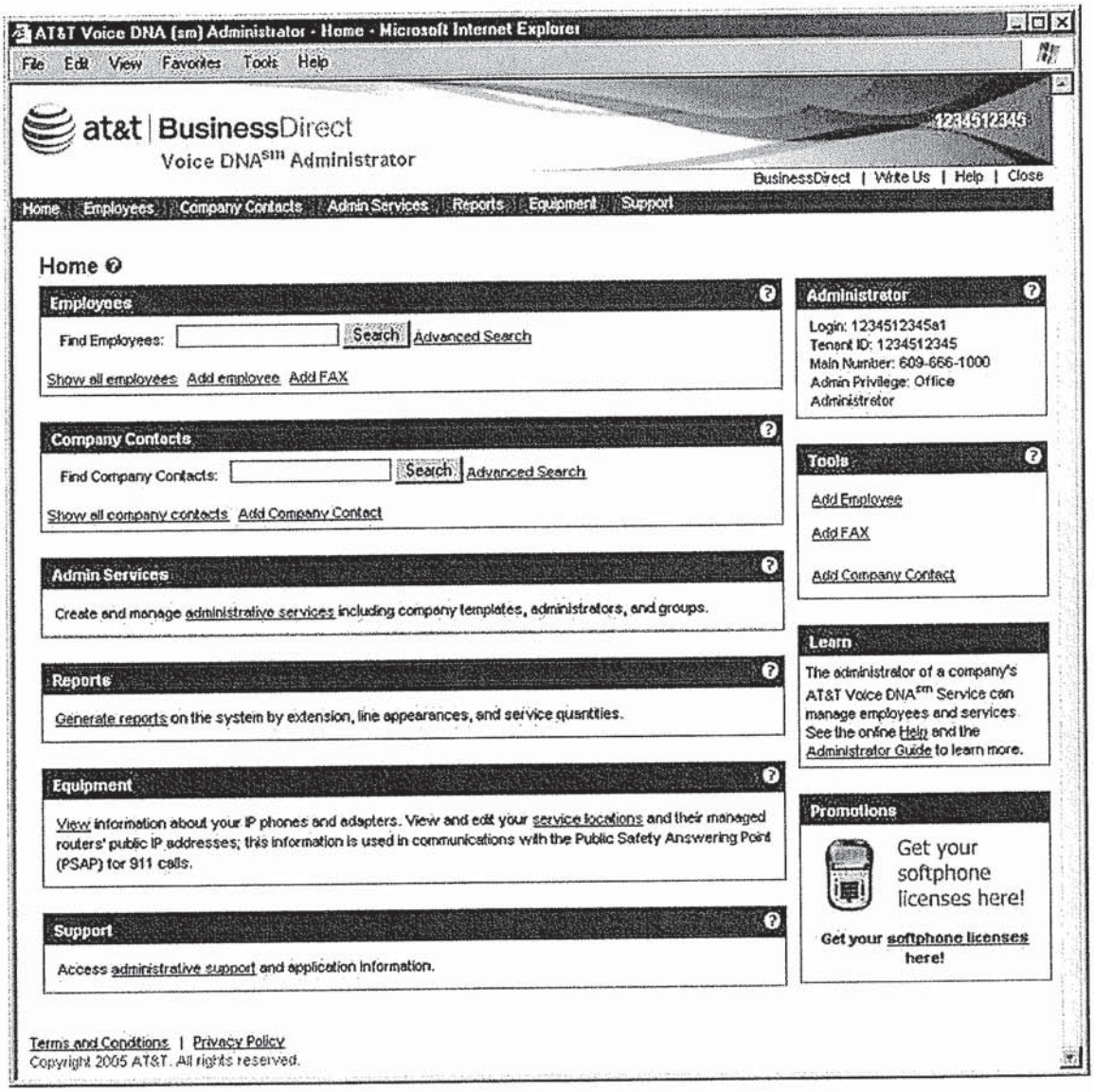
VOIP Reporting:

Web-based Tools Overview

AT&T Voice DNA®Service offers web-based tools for enterprises administrators and their end users to manage their accounts. Since the Voice DNA Administrator Tool and Personal Website are accessed via AT&T BusinessDirect®, it is best viewed with Microsoft Internet Explorer™ versions 4.0 or later. Older versions or other browsers may not allow some site elements to display or operate properly.

Administrator Tool

Customer administrators have the ability to perform MACDs Moves / Adds / Changes / Disconnects) through a separate web portal. The Administrator Tool allows administrators to pull usage reports and control feature settings such as, limiting the type and/or group of personnel with access to 8YY/9YY number dialing. An IP phone on the user's desktop provides additional functionality. These phones retain feature settings and preferences when disconnected and plugged-in at a remote location.



The following Administrator options are available:

Employee Management

- Secure Login - Password protected access to the Office Administrator (OA) portal.
- Forgotten Password Help - Lets the user obtain a new password through the system if they have forgotten their password. This page can be accessed from the login screen.
- Employees (Home Page) - Lets the OA manage day-to-day functions for business phone users.
- Employee Search - Lets the administrator perform a simple or basic search for existing employees stored in the system. *An administrator can use search criteria that includes part or all of an employee or company contact's name, phone number or abbreviated name (such as a "nickname" or abbreviated title).*
- Employee/Fax add - Lets the administrator add a new employee or fax/modem line
- Employee Portal Access - Lets the administrator access the employees' portal to perform functions on behalf of the employee
- Employee Password Reset - Lets the administrator reset the password of the employee
- Employee Extension Move - Lets the administrator move the employee's phone from one location to another.
- Employee Profile – General - Lets the administrator manage the user's name, account information, phone number information, languages, time zones, call groups and administration groups.
- Employee Profile – Company Information - Lets the administrator manage the user's company-related information
- Employee Profile – Personal Information - Lets the administrator manage the user's personal information (e.g., address, phone numbers, and email numbers)
- Employee Profile – Phone Information - Lets the administrator manage the user's phone including applying a new phone template, assigning/changing phone locations, defining bridged line appearances, defining call waiting alerting options.
- Employee Profile – Services - Allows the administrator to assign a class of service and any additional services or dialing restrictions to the user.

Company Contacts

- Contacts (Page) - Lets the administrator manage the company contact entries (excluding users) that are published to all users within the business.
- Company Contacts - Lets the OA assign contacts to the company directory and assign a favorite (speed dial) code and/or phone line key for this contact.
- Advanced Search —A search feature is available that makes it much quicker to locate a specific employee or group of employees for management purposes. The same search feature is available for company contacts, IP phones, and adapters.
- New - Lets the OA assign a contact from the company directory.
- Services (Page) - Lets the OA assign and manage various company-wide applications and services.

Administrator Services

Templates

- Phone templates – Lets the office administrator add/change/delete phone button templates for the phones used in the business.
- Classes of Service (COS) templates – Lets office administrators create class of service templates that enable services. There is a separate default COS template for each feature package. Office Administrators can create custom templates to authorize selected feature usage by an individual.

Groups

- Administration Groups – Lets the office administrator add/change/delete the administrative groups and also assign users to the groups.
- Call groups—Office administrators can create call groups that are used to limit the use of specific features such as intercom, distinctive ring, group call pickup, and directed call pickup.
- Group Administrators — Lets office administrators manage group administrators. Group administrators cannot do everything that office administrators can. Group administrators typically manage the services for a specific group of users; they cannot manage company-wide services such as hunt groups.
- Office Administrators(OA) — Lets service providers and office administrators create other office administrators, administrative groups and group administrators with all of the office administrator privileges for managing users and company-wide features.
- Hunt Groups - Lets the OA assign hunt group pilot numbers, the business extensions associated with the group and the search order for the hunt group.

Applications

- Billing Codes – Lets the administrator add/change/create the billing codes for the business.
- Adapters/IP Phones - Lets the OA/VAR view and manage client adapter settings and IP phones' extension/location information.
- Company Info - Lets the OA/VAR view and edit the information noted by the service provider about the business.
- Billing Address - Lets the OA/VAR view and edit any billing information in the event of a change of address, billing contact, etc.
- Call Distribution-tools provided for the OA to enable this function for users.
- Outlook Integration-tools provided for the OA to enable this function for users.

Reports - Generate reports on the system. See Appendix B for examples and types of reports available.

Equipment - allows OA to view IP phones, adapters, company info and billing address.

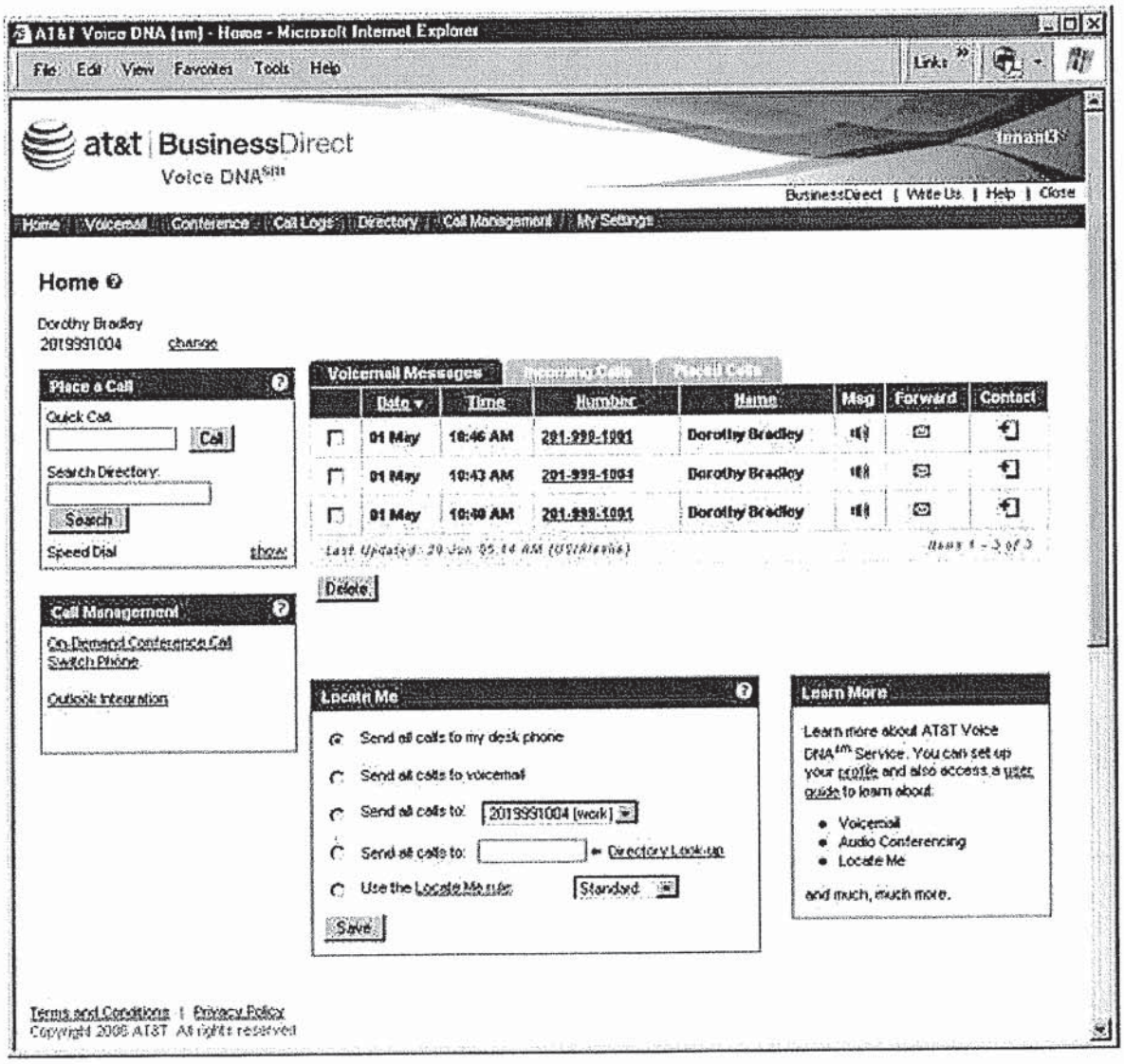
Support - access OA support and application information.

Personal Web Site

An end-user may manipulate their settings through the use of a web portal accessible from anywhere through the Internet. End-users can return voicemail messages via e-mail, listen to voicemail messages from the web site, download voicemail messages into e-mail, and review call logs via the web portal.

Apple Mac users can access the Voice DNA Personal Website using a Safari web browser version 2.0.4 running on Apple Mac OS version 10.4 to:

- Most functionality on Voice DNA Personal Website supported.
- Outlook integration NOT supported
- Access of Voice DNA Administrator Tool NOT supported
- Safari web browser on Microsoft Windows or any other configuration NOT supported.



Managed Internet Access – Optional Services

The following services are provided as options to the AT&T Managed Internet Services.

1. Option for CIPA compliant content filtering (Addresses Functional Requirement B and RFP Purpose 1-A)

Our NetTN content filtering solution is powered by Cisco, and is a cloud-based Cisco technology web security and filtering solution which has been leading the Gartner Group Leader's Quadrant for web security for the last three years. This NetTN provided Cisco Web Security solution provides a comprehensive multi-layer approach to determine whether web requests/replies are legitimate or would violate a school K-12 CIPA compliancy. Using this tool, administrators can develop and maintain content filtering policies that comply with the Children's Internet Protection Act. There are many features of our solution utilizing real time detection technologies to determine whether to block explicit web site/malicious content while passing permitted educational and business productivity content.

For additional details regarding AT&T's Content Filtering Solution, please see Functional Requirement B, Tab I "Business Plan".

2. Option for E-Mail Hosting (Addresses RFP Purpose 1-B)

AT&T Hosted Email Services

Hosted Email packs a complete personal information management system into a compact, easy-to-use interface. Business email users have different needs and requirements than personal users. Email clients like Gmail or Yahoo are great for staying in touch with friends and family, but when your business relies on email, you need more.

For Your Users

- Access to mail, calendar, contacts, tasks, and notes from one application
- Use our easy webmail client or a desktop client, like Outlook®, or Thunderbird™
- Access mail on your iPhone®, Android®, Windows® Phone or BlackBerry® device
- Optional Mobile Sync for Rackspace Webmail
- View/share/edit users' calendars
- Share calendars outside of your domain with iCal support
- Maintain and track task lists
- Create group contacts lists
- Companywide contact lists
- 25GB mailboxes
- 50MB attachments (about 500 JPEG images)
- Mail filtering controls and enhanced searching

For Your IT Department

- Easy, web-based control panel administration
- 24x7x365 support via phone, chat, or support site
- Data migration assistance available
- Industry-leading SLA
- Redundant, clustered server pairs
- Secure SSL encryption
- Add/delete/restore mailboxes from control panel
- API interface for SSO support
- Desktop client compatibility
- Domain & mailbox-level spam and virus filters
- Daily backups
- Optional email archiving service

3. Option for Web Hosting (Addresses RFP Purpose 1-C)

AT&T Web Hosting—Shared Hosting is a web service that co-exists with other websites on the same physical server, resulting in efficiencies and cost savings. However, to the world, your site looks like it exists on its own server. Shared Hosting allows you to outsource your hosting needs to AT&T. We will provision, store, and monitor your website. Shared Hosting reduces your hosting cost more than either dedicated or co-location hosting because you share secured space on a server with other customers' sites.

AT&T will assist with registering your own domain name, which becomes your unique address on the web. Once your domain name is registered, AT&T will provide you with

the space to upload your web pages to our server. When you choose Shared Hosting, you can depend on support from a provider who is committed to responsive customer service.

Premium Web Hosting	
WEB & MOBILE DESIGN TOOLS	
EasySiteWizard Pro: Choose from 1600+ templates to easily build and customize a professional website.	•
Access an advanced template gallery with 5000+ templates (manageable with popular advanced design tools like PhotoShop and Dreamweaver)	•
WordPress and Joomla Installers: Support for popular site-building and content-management tools.	•
Mobile: Create a mobile-optimized landing page.	•
Website Mobile: Build & manage a full mobile-optimized website. Includes tools to attract more mobile traffic.	Optional add-on
ECOMMERCE TOOLS	
Store Creator Pro: Build & manage a high-quality online store and securely process credit cards online	•
Shared SSL certificate, SSL Manager for transaction security	•
MARKETING TOOLS	
OneList: Business info submitted to 40+ US-based online directories.	•
SocialStream: Post to Facebook, Twitter & LinkedIn via one interface.	•
EasySiteOptimizer: Analyzes a website code and content, and provides recommendations to optimize for search engines.	•
Email Marketing Trial: Send unlimited HTML emails to a defined number of contacts. Manage campaigns & track performance.	50 contacts
Web Analytics: Track website traffic, referral sources and more.	•
EMAIL FEATURES:	
Professional email featuring IMAP/POP, web-based mail, antivirus/ spam filtering and collaboration tools to share calendar and contacts.	500 accts. (2 GB each)
HOSTING FEATURES:	
Web storage and data transfer	Unlimited
Number of domain names supported	10
MSSQL database management - Storage	2 @ 200 MB
MYSQL database management	Unlimited
FTP – number of users	500
Web alias	Unlimited
Basic hosting features: Access to Log Files, Archive Manager,	•

Content Support - Dynamic, CP Site Map, PHP MyAdmin, Disk Usage Meter, DNS Manager, Domain Manager, File Manager Pro, File Extraction, FTP Manager, FTP Access (AFTP/SFTP/FTPS), Log Manager, Raw Log Files, Secure Shell (SSH), Password Protect Web Directories, Perl 5, Perl Scripts Checker, PHP 5, CGI Script
Advanced hosting features: MS FrontPage Manager, Windows Services Manager, ADO.net, ASP / ASP.net, C/C++, ColdFusion / ColdFusion MX, Cron Support, GCC, GD Library, IIS ASP Components, ImageMagick, IonCube Loader Support, JSP™ Support, Microsoft® Access, Own CGI Bin, Python, Ruby, Server Side Includes (SSI), TCL, XML Parser, Zend Optimizer Support, Anonymous FTP.

B. Technical Requirements for Content Filtering of Managed Internet Access

The vendor must propose a solution for content filtering which is compliant with the Children's Internet Protection Act (CIPA). Information for this may be obtained from the USAC website. There will be separate pricing required for this service on the cost section of the RFP.

This filter service will be optional for LEAs to accept with the Managed Internet Access from the awarded provider.

AT&T Response:

Our NetTN content filtering solution is powered by Cisco, and is a cloud-based Cisco technology web security and filtering solution which has been leading the Gartner Group Leader's Quadrant for web security for the last three years. This NetTN provided Cisco Web Security solution provides a comprehensive multi-layer approach to determine whether web requests/replies are legitimate or would violate a school K-12 CIPA compliancy. Using this tool, administrators can develop and maintain content filtering policies that comply with the Children's Internet Protection Act. There are many features of our solution utilizing real time detection technologies to determine whether to block explicit web site/malicious content while passing permitted educational and business productivity content. The solution provides:

1. Web Filtering with Active Directory integration
2. Application Control

3. Web Malware Scanning
4. Superior Reporting
5. Ability to create different access policies based on organizational structure
6. Category based web filtering with 78 categories
7. Customizable block and allow filter list
8. Dynamic categorization of web pages
9. Customizable block pages per K-12 district
10. Keyword blocking within forum posts and web-based chat
11. Customizable dictionary
12. Safe-search enforcement and advanced Search*ahead* feature displays search results in different risk categories
13. Ability to apply quotas to web traffic bandwidth per group
14. Centralized policy management and strong reporting web portal to provide ease of use for policy configuration and analytic reporting/auditing. Granular reporting enables actionable remedies to issues and unrivalled visibility into resource usage
15. 10,000+ report combinations covering more than 100 attributes in 11+ reporting categories
16. Scheduled reports can be sent securely to defined users
17. Cumulative, trending and search driven forensic reports, comprehensive drill down analysis

The NetTN web security solution has 78 comprehensive granular categories which help to minimize overlap of URLs into more than one category, includes web anti-virus/anti-malware protection, and includes Safesearch Enforcement with *SearchAhead* early warning filtering of search results and Web 2.0 application control; all of these helping against the ever changing Internet application threats. Many non-NetTN solutions are lacking these protective features to enforce CIPA compliancy for the K-12 districts. Further many non-NetTN solutions are also lacking these protective features to enforce CIPA compliancy and forcing the filter to over-block/under-block legitimate/illegitimate

web content. For example, many non-NetTN solutions may filter only by URL categories and SafeSearch enforcement but not providing *SearchAhead* real-time early warning filtering/identification. The NetTN web security solution's *SearchAhead* feature will further filter illegitimate search results that were not correctly classified by a web provider's Safesearch enforcement engine. Additionally, most of the non-NetTN solutions will consist of a lot of categories (e.g. over 85) with causes overlapping of URL/Content in different categories. This can create a daunting task for an administrator to block obscene URL/Content that may overlap in both legitimate and illegitimate categories. To mitigate this, some non-NetTN web filters require their administrators to block both categories and then build a custom allow list of URLs/Content from the legitimate category. In contrast, the NetTN web security solution utilizes a rule precedence method in which if the first rule blocks the illegitimate category then all URL/Content in the category will be blocked.

URLs/Content, web 2.0 application/widgets that are visually obscene, child pornography or information harmful to minors are placed in the high risk categories such as pornography, hate/racism, weapon, illegal drug, etc. Blocking these high risk categories will provide protection against illegitimate websites/content. The NetTN web security's URL/Content filtering solution not only provides you the ability to block these sites but will provide in-depth analytic reports of category hits by user/group/IP address.

The NetTN web security solution can be integrated with K-12 school's LDAP directory service (e.g. Windows Active Directory, Novell Directory Service) or SAML 2.0 iDPs (e.g. Windows Active Directory Federated Service) to provide user/group level granularity. Utilizing the user/group AD access control, the NetTN web security solution allows the administrator to create policies for Teachers/Administrators who are engaged in research while still maintaining the blocking of student user group from gaining access to research site, if desired. Using the K-12 Directory service/Federated service provides a single sign-on feature where user/group only needs to log-on to their AD domain which forwards user/group information to the NetTN web security solution. Once the AD user/group information is in the NetTN web security solution, the TC administrator will be able to configure/create content filtering based on the district's AD user/group credentials.

For example, the administrator can create polices that only allows teacher/research to restricted sites for research purposes. Also, a hard limit expiration timer can be set on how long a user/group can surf to restricted sites. Expiration timers can be configured in AD to limit the user/group access out to the Internet or in the NetTN web security solution with a time based user/group filter policy.

All user/group web activities are logged separately and stored at the data center reporting repository. The data center will store historical data online for a year, and any older data will be kept and archived. The NetTN web security solution provides in-depth visibility into the web activity logs by using a state of the art web intelligence reporting engine. With this reporting engine, administrators can create an unlimited amount of custom or composite reports based on over 100 specific attributes. Reports can be generated into multiple formats and built using graphical pie charts and/or graphing. The NetTN web security solution's reporting engine also offers customers the ability to schedule reports which can be automatically sent to a requested group of administrators on a daily, weekly or monthly basis.

The NetTN web security solution supports both RFC 1918 private addressing and RFC 1631 Nat'ed/Pat'ed addressing.

The NetTN web security's content filtering solution supports block page customization. Notification Block pages/messages can be done using standard HTML tag or just plain text. Parameter such as #category, #username, #URL and #reason are used to identify the category getting block, the username, the URL getting blocked and the reason for the block notification.

Further detail of these NetTN web security layers are outlined below:

1. The NetTN web security solution incorporates global intelligence web site categorization heuristics which utilizes multiple techniques such as real time dynamic content classification, an industry-leading reputation database system and file type filters. The NetTN web security solution has visibility into over 20 global datacenters whose sole purpose is to filter web traffic and identify malicious web traffic around the world. This enables the NetTN web security's filtering to benefit from a massive information database about web content sources and risks gathered across the entire Internet. The system builds a category based filtering repository/database that experiences over 20 billion web requests per day and benefits from identifying/blocking over 7 billion instances of malicious content per day. Web site categorization and malicious web content classification is done in real time thus allowing the NetTN web security solution to be abreast of changing Internet web sites and threats.

   The NetTN web security solution's reputation rating method used by the database is analogous to the manner in which a credit agency provides credit scores to enable reliable commerce. The URL/Content reputation scores for websites, domains, or IP addresses, are based on known behaviors from a legitimate web source, including deviations from expected behaviors, and dynamic assessment of security risks. Using this real-time scoring, the filter proactively and reliably

detects URLs/web content that are categorized as non-CIPA compliant by your school district's policy.

The NetTN web security solution will filter content based on URL/IP address or HTTP/HTTPS traffic. Filtering URL/Content may require you to block a specific category but at the same time allow a legitimate URL/Content from within that same blocked category. This can be a daunting task for many filtering solutions; however the NetTN solution will provide you the option to create rules/policies that utilize the predefined URL/Content categories and to customize allow/block lists of URL/IP addresses at the same time.

2. The web security component of the NetTN solution further protects users from web viruses and malware. The solution utilizes Artificial Intelligence heuristics (e.g. neural network, Bayes Naive) learning software call "scanAllows" to analyze all elements (e.g. HTML, Java Script, Flash and Active Script) to build a detailed view of each web site request and any associated virus/malware security risk. Results from the web site elements and ScanAllows are further analyzed in a meta scanner to determine/identify the security posture of the web request/site. Upon identifying the web security risk, the system will classify and block web site element from contaminating school PCs/Hosts system. Visibility of virus/malware can be seen in the system reporting dashboard or the School TC admin can create scheduled reports on virus/malware which were identified by the NetTN Web security system.
3. The solution provides filtering for Web 2.0 applications and widgets such as social media, social networking and SaaS applications. Web 2.0 application and their widgets utilize port 80 and 443 to communicate with external application service providers. Social Networking Web 2.0 such as Google or Facebook have very useful/productivity application widgets for K-12 districts, however as there are many productivity Web 2.0 widgets, you will find a similar amount of non-productivity application widgets from these social network sites. You can use the NetTN solution's Application Control function to block access to inappropriate web 2.0 applications/widgets thus mitigating web 2.0 application security risks or prevent applications from draining K-12 classroom productivity. Additionally, the NetTN web security solution dynamically updates its Web 2.0 application signatures to remain current with the constantly updating and changing nature of Social Media/Social Network applications/widgets.
4. The NetTN solution enforces Safe Search on a per school district or IP range basis. An Internet search engine can often return results that are non-CIPA compliant based on the settings of the end user's PC browser's preference/setting page. To make sure that search results comply with school policy, the safe search setting /preference must be user or system-configured to the "strict" setting. In the

event of an improper PC browser safe search setting or misconfiguration, our solution will ensure that Safe Search enforcement is enabled.

Enabling/Enforcing a search engine's safesearch feature does not necessary block all the explicit sites or malicious content from your search results as those results are up to the search providers (.e.g. Google, Yahoo, Bing). Recognizing this, the NetTN web security solution's SearchAhead feature was developed to provide early warning and real time scanning of search engine results to identify any inappropriate or malicious content the search engine safe search feature was not able to detect. The Search Ahead feature works in conjunction with our web categorization engine and web anti-Virus/anti-Malware detection to flag the search results in real time thus mitigating search result non-CIPA compliant risks against school policy.

C. Technical Requirements for Managed VoIP

Managed VoIP is the ability to use the Internet Protocol (IP) to place voice calls and transport voice traffic over the data network,

A solution based on services provided by a telecommunications provider that is primarily based on traditional monthly usage charges for tariff or contracted telephone services with little or no customer owned equipment. This may be based on Centrex, Plexar, POTS or other telephone services

It must be a turn-key solution and must be consistent with current E-Rate ELS funding and eligibility guidelines.

The solution must include:

9. Adds, moves and changes to end user telephony setup

AT&T Response:

For the prices quoted herein, AT&T will provide only the items of equipment and services specifically listed in this response. Any additional equipment or services beyond those herein will be provided at additional charge(s). AT&T's pricing is predicated on the requirements as set forth in the RFP document and AT&T's response. Use of the word "turnkey" or similar terms does not require AT&T to provide equipment or services beyond those specifically quoted in this RFP response. AT&T will follow all Service Provider requirements for the USF Schools and Libraries Program as set forth on the USAC website and FCC rules.

AT&T provides other Priority 1 voice services including, but not limited to, PRI, Centrex, and business lines (POTS) in Tennessee. These services are currently deployed for many school systems and school districts throughout the state, and they are readily available in AT&T's service footprint.

- Primary Rate Interface (ISDN PRI) is a voice and data service that provides high-volume access to the public switched telephone network (PSTN). ISDN PRI provides 23 digital channels over one transport line (a 24th channel carries signaling information). This service offers one T1 circuit with 23 separate voice lines or a combination of services.
- Centrex is a dial tone service that provides features and functions commonly associated with expensive PBX equipment, but the features and functionality are housed in the AT&T central office providing an inexpensive voice solution.
- AT&T's business lines provide Plain Old Telephone Service (POTS).
- AT&T also provides the following Voice over IP service as a priority offering.

AT&T Voice Over IP

AT&T Voice DNA (IP Centrex) is a network-based, fully hosted VoIP solution that offers businesses a full range of advanced calling features, applications, and management tools for employees and remote workers over a single network interface.

AT&T Voice DNA Offers:

- Delivered over IP Connection (AT&T Managed Internet Service)
- All-Distance Calling
- Telephone features and enhanced applications
  - Voice Mail
  - Locate Me (Find Me/Follow Me)
  - Conferencing on Demand
  - Auto Attendant
  - End User and Administrator Portals
  - Customized – Focus group tested
  - All applications integrated into a single front page via AT&T BusinessDirect℠
  - Highly Secure > Single Login; Exceeds Security standards
- Customer Premises Equipment

- Interoperability Test Lab to ensure phones are compatible
- Automated SIP Phone provisioning and plug & play registration/configuration
- Automated firmware updates to ensure phones have latest upgrades/patches
- Soft Phone Support
- CPE Design, Install, and Installation Support

- Benefits
  - Support for Remote and Nomadic Workers
  - Greater Business Productivity
  - Reduced Complexity
  - Cost Savings

Service Description

AT&T Voice DNA provides a network-hosted, Session Initiation Protocol (SIP)-based communications solution. Voice DNA leverages AT&T provided access, converging voice and data applications over one connection, providing our customers with carrier-class features such as:

- primary local calling features: N11, 8YY, PSTN off-net;
- line-side features: Call Hold, Call Waiting, Conferencing; and
- advanced features: Locate-Me, on-demand audio conferencing, Auto Attendant and Queuing capability

Voice DNA is provided via a network Application Server (AS) platform that serves as the virtual, hosted IP PBX, providing line-side features on top of carrier-class local services and features. All Voice DNA originated calls access the Voice DNA AS for determination of customer calling features, etc. and provides the following capabilities:

- Support of line side and advanced features
- Support of add-on optional ('a la carte') features
- Administrator Tool-Centralized management of the Voice DNA Service
- Personal Web Site-end user call management
- Support of VoIP administered private dialing plans by completing internal calls within the "Voice DNA Application" and routing all other calls to the VoIP Network Infrastructure
- IP Phone Automated Registration
- Support for Virtual Telephone Numbers (VTNs)

- Operations, Administrative and Maintenance functions

Voice DNA eliminates the need for a PBX or IP PBX on the customer's premises. Delivering consistent feature/functionality that is available at corporate headquarters to remote sites has traditionally been a challenge for multi-location businesses. Since Voice DNA is network based, access for remote offices is easily achieved, with a variety of access types supported. Virtually any location can be connected, offering the full range of features.

Multiple end user devices including IP phones and soft phones have been certified for interoperability – allowing calls to be placed or received to/from users at the same site, to/from users at different VoIP enabled sites and to/from users connected to the PSTN.

Voice DNA requires that the "hub" site (site with dedicated access) must utilize one of the AT&T managed IP services.

AT&T Voice DNA® E911

There are some critical differences between E911 (Enhanced 911) services using AT&T Voice DNA® services (Voice over IP) and 911 using traditional phone services. Inaccurate or incomplete data of the caller's location will not allow the E911 system to pinpoint the location of the user and has the potential to foil an emergency rescue and put the caller's life at risk. The FCC has issued an order which requires service providers to implement a solution that will be able to pinpoint the location (The service room number/floor of the phone in 4Q '10 if supported by the Public Service Answering Pont (PSAP)) of the user. In addition, the provider must notify customers about 911 services over the IP network and obtain customer acknowledgement of receipt of this information.

Feature Packages Overview

Voice DNA Service offers three feature packages and several optional features. The following table summarizes the packages and optional features (subject to change based on availability for Controlled Introduction/General Availability). All packages include BusinessDirect Portal and Administrator Tool.

Standard (No Personal Web Site)	Enhanced (With Personal Web Site)	Premium (With Personal Web Site)	Optional Features (Orderable with Enhanced and Premium Packages)
Abbreviated Dialing	STANDARD	ENHANCED	Audio conferencing (up to 10 users) Per

Standard (No Personal Web Site)	Enhanced (With Personal Web Site)	Premium (With Personal Web Site)	Optional Features (Orderable with Enhanced and Premium Packages)
• Intra tenant • Bi-Directional-VDNA/NON-VDNA Users Audible Call Forward Auto Callback Busy Call Waiting-Block/Unblock Caller ID Presentation Caller Name and Number Presentation Caller ID Blocking per Call Caller ID Blocking for all calls (with override) Call Forward – Busy (via star code) Call forward – No Answer (via star code) Call Hold Call Reason Display Call Restriction Call Transfer – Blind Call Transfer - Consultative Custom 911 Routing Dial "0" for Company Operator DID (Direct Inward Dialing) DOD (Direct Outward) External Transfer Executive Busy Override Fax machines utilizing G.711 Fax protocol Last Number Redial Music on Hold-(ON/OFF)	PLUS: <u>Personal web site features:</u> Click to Call Call Logs Missed Call Notification Locate Me Call Forward- Busy Call Forward – No Answer Call Forward - Variable Call Treatments Caller Categories (Groups) Simultaneous Ring No Answer Ring Timers Selective Call Forwarding Selective Call Rejection from callers in specific call categories Selective Call Acceptance Call Forking Speed Dialing Corporate Speed Dialing Personal (Favorites) Directory/Contacts Alternate Name Search My Profile <u>Phone Features:</u> Bridged Line Appearance	PLUS: Outlook Integration Voicemail (with UM, Message waiting light, zero-out option, e-mail and pager notification, AT&T wireless integration) Switch Phone	Seat Auto Attendant Call Distribution Module Site Survivability

Standard (No Personal Web Site)	Enhanced (With Personal Web Site)	Premium (With Personal Web Site)	Optional Features (Orderable with Enhanced and Premium Packages)
• Caller suppression of MOH • Music selection • Customized with announcements • Choice at user, group or tenant level Ringdown/Hotline Station to Station Dialing Three-way Conferencing	Multiple Line Appearances-single extension Multiple Line Appearances–multiple extensions Call Forwarding - Unconditional Call Park Call Pick-up Call Pickup- Directed Call Pickup- Group Click to Call LCD Distinctive Ringing Intercom Calling Do Not Disturb Last Call Return <u>Common Capabilities:</u> Account Codes – Mandatory Account Codes – Optional Call Groups Hunt Groups • Choice of Ring Sequences • Option to loop ringing sequence		

Optional Features

The following features are available for an additional charge to Enhanced and Premium subscribers. These features are also dependent upon the phone/handset selected.

Audio Conferencing

Provides on-demand (click-to-conference) conference calls for up to 10 participants via web portal and up to 3 participants via phone. Mandatory Account Codes supported on

click-to-conference calls. Please note this is a not a reservation service, it is on-demand initiation only.

Auto Attendant

Also known as **Call Tree** allows calls to be routed using responses provided by users via a touch-tone telephone. Callers connected to an Auto Attendant hear customer-provided voice menus and make selections between options so that their call is routed to selected extensions, departments, voice mailboxes, prerecorded information or announcements. This feature also allows customers to direct calls that are inbound to their 8YY telephone services to be terminated at the VDNA Auto Attendant.

The recording of greetings, announcements, and prompts must be performed by the customer. The recording is accomplished using the Auto-Attendant's telephone-based tool. Auto Attendant permits up to three levels of menu options, each consisting of up to seven choices ("7 x 7 x 7").

The customer may have multiple Auto Attendants per site. The Customer Administrator must assign one or more VDNA telephone numbers as the Call Tree Number (CTN). This number comes from the block of numbers the customer requested for the Voice DNA service. One of these numbers must be designated as the **Primary CTN**. Customers have the option of assigning New AT&T provisioned telephone numbers or porting a telephone number they currently use for their existing auto attendant. In addition to the Primary CTN, an Auto Attendant can be assigned up to fifteen (15) "Alias" numbers also known as "**Secondary CTNs".** These also come from the customer's block of VDNA numbers.

Customers must order the quantity of Auto Attendants they wish to provision per site and the maximum number of Simultaneous Calls that are to be permitted across **ALL** Auto Attendants ordered at this site. Note that we will be monitoring the customer's simultaneous call usage monthly. If the usage is consistently over the subscribed capacity, the customer will be asked to increase the number of simultaneous calls. The Auto Attendant order should be placed along with the Voice DNA site order.

Pricing for Auto Attendant consists of two elements:

Auto Attendant Set Up Fee –a one-time (Non Recurring) fee per Auto Attendant per Site (this fee is not discountable and cannot be waived)

Auto Attendant Monthly Recurring Charge – per Simultaneous Call capacity ordered by customer for Auto Attendants provisioned at a Site. There is a minimum of 4 Simultaneous Calls

Customers who have Auto Attendant are provided with access to the ECAT tool which displays views of the Auto Attendant/Call Tree structure including settings, daily schedules, global events and a list of their prompts (also called nodes). ECAT allows for modification to the following parameters:

- Change prompt recordings
- Change Phone Numbers for transfer destinations
- Ability to add/remove names from the Dial by name/Extension directory. Names can be spelled "phonetically" so Text To Speech (TTS) will pronounce correctly.
- Change Admin PIN – this is the PIN associated with the Auto Attendant Telephone User Interface (TUI)
- Emergency Greeting – to set-up/turn-on emergency greeting that will be played prior to playing the current Auto Attendant schedule
- Override Schedules – to temporarily change an Auto Attendant schedule, i.e., after hours, holiday, etc.
- Manage Global event setting

The tool requires a separate Login and Password – to be provided when Auto Attendant is delivered to the customer.

Call Distribution Module

Call Distribution provides an affordable ACD (Automated Call Distribution) function where callers are queued for answering by representatives who enter and exit the queue on their own. For example, Call Distribution can be used for a customer support group, agents taking reservations, or agents making appointments. For customer service, your customers with support contracts can be given a specific support number, which is the Call Distribution telephone number.

Customer support representatives can then check themselves in or out of the Call Distribution call answering queue.

You can configure up to 50 Call Distribution Modules or queues per tenant ID that can have up to 200 representatives at any given time.

Office administrators can create multiple Call Distribution queues. When multiple queues have been created, representatives check themselves into a specific queue by entering the pilot number (extension) for the queue and an optional pass code if one is specified. You can also specify the number of callers allowed in the queue, the number of agents that can

be checked into the queue at one time, and the announcement/music file that should be played for callers to the specified queue.

Additionally, AT&T provides the capability for a customer to add a customized announcement. The customer sends in their unique text announcement, AT&T records it and mixes it with the standard music on hold. Each recorded announcement will use the same music clip provided by AT&T. All announcement files will be .WAV files. The maximum length of the announcement is 5 minutes. The default announcement is not considered a customized announcement. Customers will be limited to 4 customized announcements per queue ordered. This limit is called the 'Call Distribution announcement quota'. Customers will be limited to 3 announcement changes on a monthly basis. This limit is called the customer's 'Call Distribution change quota'. The deletion of an announcement does not count against the customer's Call Distribution change quota. The Call Distribution announcement and change quotas will be set based on the number of queues ordered, but enforced as a single number against all queues. The Call Distribution change quota will be reset based on the calendar month. The Call Distribution change quota will not be pro-rated if Call Distribution is ordered mid-month. Service Delivery and Customer Care agents with the roles of 'Master' or 'Full' are the only agents allowed to update announcement status via the customer care portal. The customer must contact Customer Care if the Call Distribution change quota has been exceeded and an additional request is needed.

After the Test and Turn-up for the Customized Announcement has been completed, the customer will contact Customer Care (Service Assurance) if:

- There is any trouble with the announcement or
- The customer is not satisfied with the announcement or
- Needs re-instatement of a de-activated announcement

Call Prompter features can also be provided with the Call Distribution Module by subscribing to the Auto Attendant (optional feature).

This is an affordable ACD. It is not what is often considered a full function ACD, as the following features are not currently supported:

- Time of Day Routing
- IVR-Interactive Voice Response
- Recording or Barging

VoIP Demarc/Site Survivability

VoIP Demarc/Site Survivability is a required feature of AT&T Voice DNA service on AVPN but is optional for AT&T on MIS/PNT.

VoIP Demarc/Site Survivability is provided by deploying an EdgeMarc device, also called the AT&T Managed Integration Device (MID), at the customer's premises. The MID functions as the service demarcation point for Voice DNA on AVPN. The MID is managed by AT&T. The MID's role as a demarcation device is to allow AT&T to manage the customer's Voice DNA network based service. Management includes:

- Maintenance of EdgeMarc MID.
- 911 move detection & restriction
- Performance reporting
- Site Survivability (optional) via POTS or PRI access to the MID

VoIP Demarc/Site Survivability Option provides continuity of AT&T VDNA® service in the event of a failure of a customer's connectivity to the AT&T network by routing calls over the Public Switched Telephone Network (PSTN). This service is offered as an optional feature for VDNA on MIS/PNT and for VDNA on AVPN it is required but implementing the Site Survivability feature is optional.

This option provides call routing under 3 scenarios:

- On-LAN calls [off-site]
- Off-LAN calls over POTS or PRI (VDNA on AVPN only) lines to PSTN network
- Incoming calls on POTS or PRI (VDNA on AVPN only) lines routed to the location's Default Calling Number (DCN)

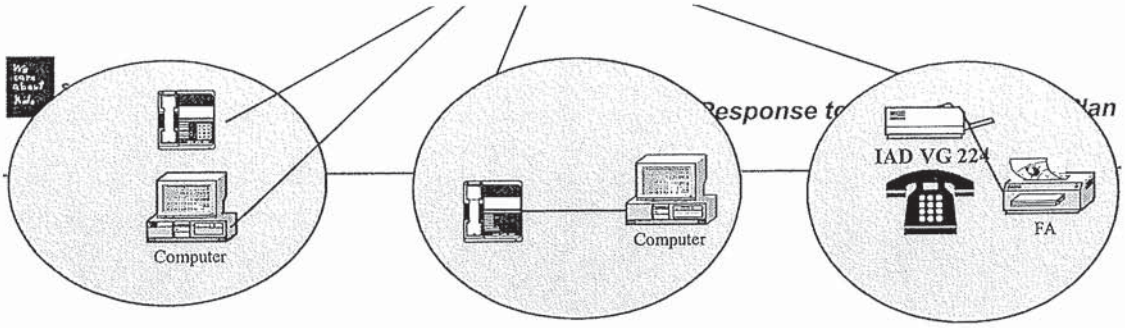
This functionality is provided by an AT&T-managed EdgeMarc device installed on the customer site between the managed router and the LAN switch. Two EdgeMarc Models are supported:

- Model 4508T4W - 2 FXO ports and 6 FSX ports
- Model 4562T4W - 6 FXO ports and 2 FSX ports
- Model 4608T4W - 2 FXO ports and 6 FSX ports (only available with VDNA on AVPN)

FXO ports are used for failover to the PSTN and FXS ports are for analog phone adapters (phone or fax). All FXO ports on a device must be enabled with a POTS or PRI (VDNA on AVPN only) connection.

Site Survivability Configuration

This diagram shows a typical configuration using the Site Survivability feature.



The EdgeMarc device is configured and staged by the vendor (Edgewater Networks) per customer's specific LAN configuration and shipped to client's site. The device must be installed by AT&T or an AT&T subcontracted installer. The charge for installation is included in the VoIP Demarc/Site Survivability Set Up Fee. AT&T (or a contractor of its choosing) will perform the installation of the AT&T Voice DNA service, including the EdgeMarc Device with Site Survivability feature enabled at the Customer site if requested. For Voice DNA on MIS/PNT this feature may be ordered and installed at the time of initial Voice DNA service turn-up or added to an existing Voice DNA service.

VoIP Demarc/Site Survivability is an optional feature with the AT&T Voice DNA® Service on MIS/PNT but is required with AT&T Voice DNA® on AVPN. Customers must select from an AT&T certified list of EdgeMarc devices appropriate for their business. Pricing for Demarcation/Site Survivability consists of two elements:

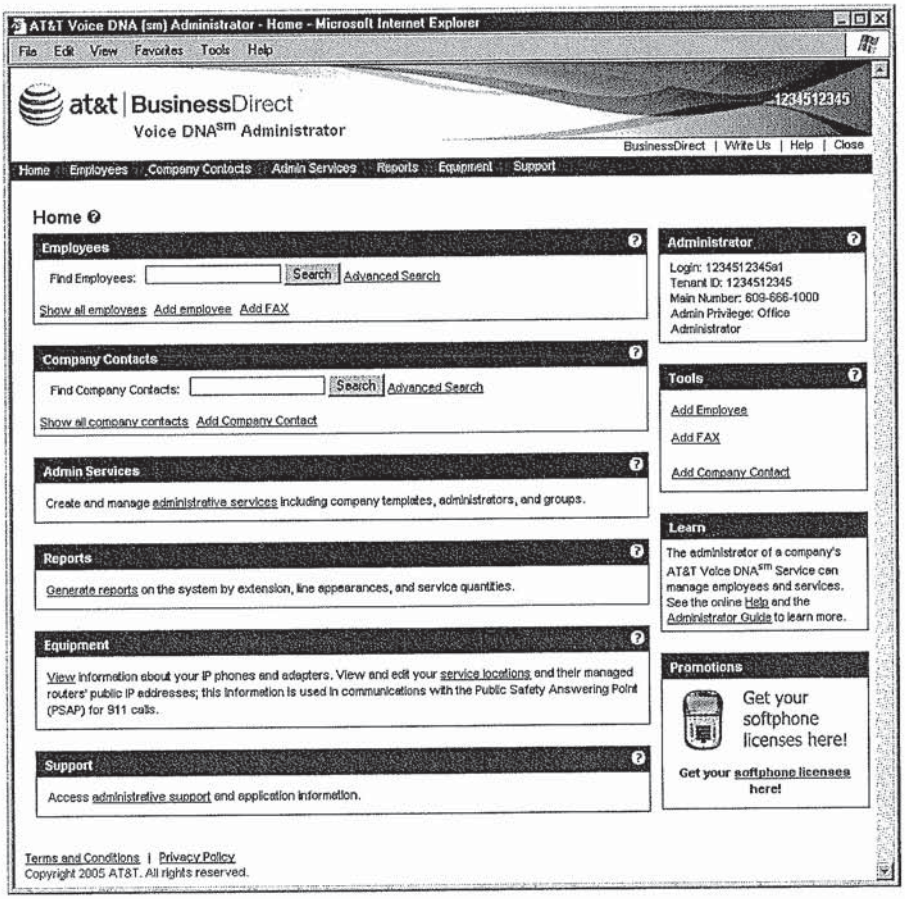
- VoIP Demarc/Site Survivability Set Up Fee – charged as a one-time (Non Recurring) fee per Site.
- VoIP Demarc /Site Survivability Monthly Recurring Charge – per Site.

Web-based Tools Overview

AT&T Voice DNA®Service offers web-based tools for enterprises administrators and their end users to manage their accounts. Since the Voice DNA Administrator Tool and Personal Website are accessed via AT&T BusinessDirect®, it is best viewed with Microsoft Internet Explorer™ versions 4.0 or later. Older versions or other browsers may not allow some site elements to display or operate properly.

Administrator Tool

Customer administrators have the ability to perform MACDs Moves / Adds / Changes / Disconnects) through a separate web portal. The Administrator Tool allows administrators to pull usage reports and control feature settings such as, limiting the type and/or group of personnel with access to 8YY/9YY number dialing. An IP phone on the user's desktop provides additional functionality. These phones retain feature settings and preferences when disconnected and plugged-in at a remote location.



AT&T Voice DNA® Administrator Web Tool

The following Administrator options are available:

Employee Management

- Secure Login – Password protected access to the Office Administrator (OA) portal.
- Forgotten Password Help – Allows the user obtain a new password through the system if they have forgotten their password. This page can be accessed from the login screen.
- Employees (Home Page) – Allows the OA manage day-to-day functions for business phone users.
- Employee Search – Allows the administrator perform a simple or basic search for existing employees stored in the system. An administrator can use search criteria that includes part or all of an employee or company contact's name, phone number or abbreviated name (such as a "nickname" or abbreviated title).
- Employee/Fax add – Allows the administrator add a new employee or fax/modem line
- Employee Portal Access– Allows the administrator access the employees' portal to perform functions on behalf of the employee
- Employee Password Reset– Allows the administrator reset the password of the employee
- Employee Extension Move – Allows the administrator move the employee's phone from one location to another.
- Employee Profile – General - Allows the administrator manage the user's name, account information, phone number information, languages, time zones, call groups and administration groups.
- Employee Profile – Company Information - Allows the administrator manage the user's company-related information
- Employee Profile – Personal Information - Allows the administrator manage the user's personal information (e.g., address, phone numbers, and email numbers)
- Employee Profile – Phone Information - Allows the administrator manage the user's phone including applying a new phone template, assigning/changing phone locations, defining bridged line appearances, defining call waiting alerting options.
- Employee Profile – Services – Allows the administrator to assign a class of service and any additional services or dialing restrictions to the user.

Company Contacts

- Contacts (Page) – Allows the administrator manage the company contact entries (excluding users) that are published to all users within the business.
- Company Contacts – Allows the OA assign contacts to the company directory and assign a favorite (speed dial) code and/or phone line key for this contact.
- Advanced Search – A search feature is available that makes it much quicker to locate a specific employee or group of employees for management purposes. The same search feature is available for company contacts, IP phones, and adapters.
- New – Allows the OA assign a contact from the company directory.
- Services (Page) – Allows the OA assign and manage various company-wide applications and services.

Administrator Services

Templates

- Phone templates – Allows the office administrator add/change/delete phone button templates for the phones used in the business.
- Classes of Service (COS) templates – Allows office administrators create class of service templates that enable services. There is a separate default CoS template for each feature package. Office Administrators can create custom templates to authorize selected feature usage by an individual.

Groups

- Administration Groups – Allows the office administrator add/change/delete the administrative groups and also assign users to the groups.
- Call groups—Office administrators can create call groups that are used to limit the use of specific features such as intercom, distinctive ring, group call pickup, and directed call pickup.
- Group Administrators – Allows office administrators manage group administrators. Group administrators cannot do everything that office administrators can. Group administrators typically manage the services for a specific group of users; they cannot manage company-wide services such as hunt groups.
- Office Administrators(OA) – Allows service providers and office administrators create other office administrators, administrative groups and group administrators with all of the office administrator privileges for managing users and company-wide features.

- Hunt Groups – Allows the OA assign hunt group pilot numbers, the business extensions associated with the group and the search order for the hunt group.

Applications

- Billing Codes – Allows the administrator add/change/create the billing codes for the business.
- Adapters/IP Phones – Allows the OA/VAR view and manage client adapter settings and IP phones' extension/location information.
- Company Info – Allows the OA/VAR view and edit the information noted by the service provider about the business.
- Billing Address – Allows the OA/VAR view and edit any billing information in the event of a change of address, billing contact, etc.
- Call Distribution-tools provided for the OA to enable this function for users.
- Outlook Integration-tools provided for the OA to enable this function for users.

Reports - Generate reports on the system. See **Appendix B** for examples and types of reports available.

Equipment - allows OA to view IP phones, adapters, company info and billing address.

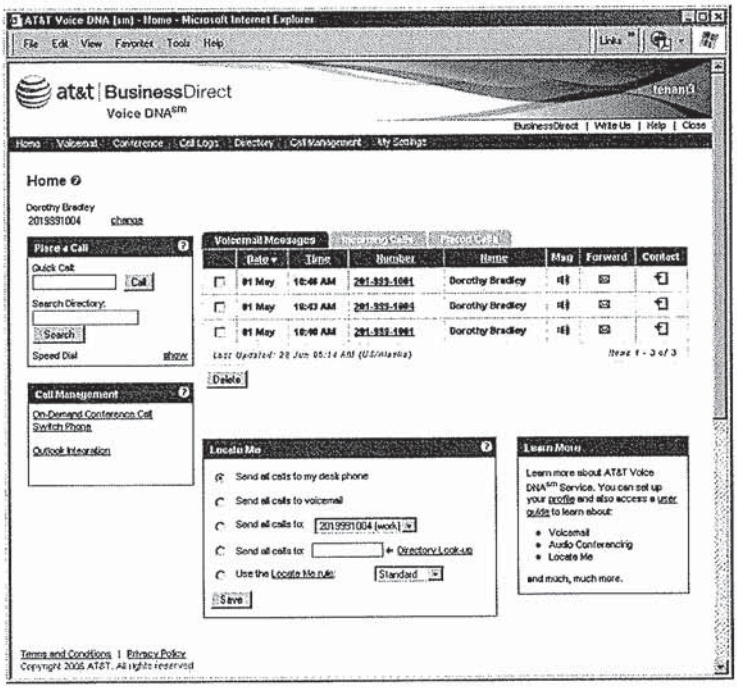
Support - access OA support and application information.

Personal Web Site

An end-user may manipulate their settings through the use of a web portal accessible from anywhere through the Internet. End-users can return voicemail messages via e-mail, listen to voicemail messages from the web site, download voicemail messages into e-mail, and review call logs via the web portal.

Apple Mac users can access the Voice DNA Personal Website using a Safari web browser version 2.0.4 running on Apple Mac OS version 10.4 to:

- Most functionality on Voice DNA Personal Website supported.
- Outlook integration NOT supported
- Access of Voice DNA Administrator Tool NOT supported
- Safari web browser on Microsoft Windows or any other configuration NOT supported.



AT&T Voice DNA® Personal Web Site

Managed IP Access

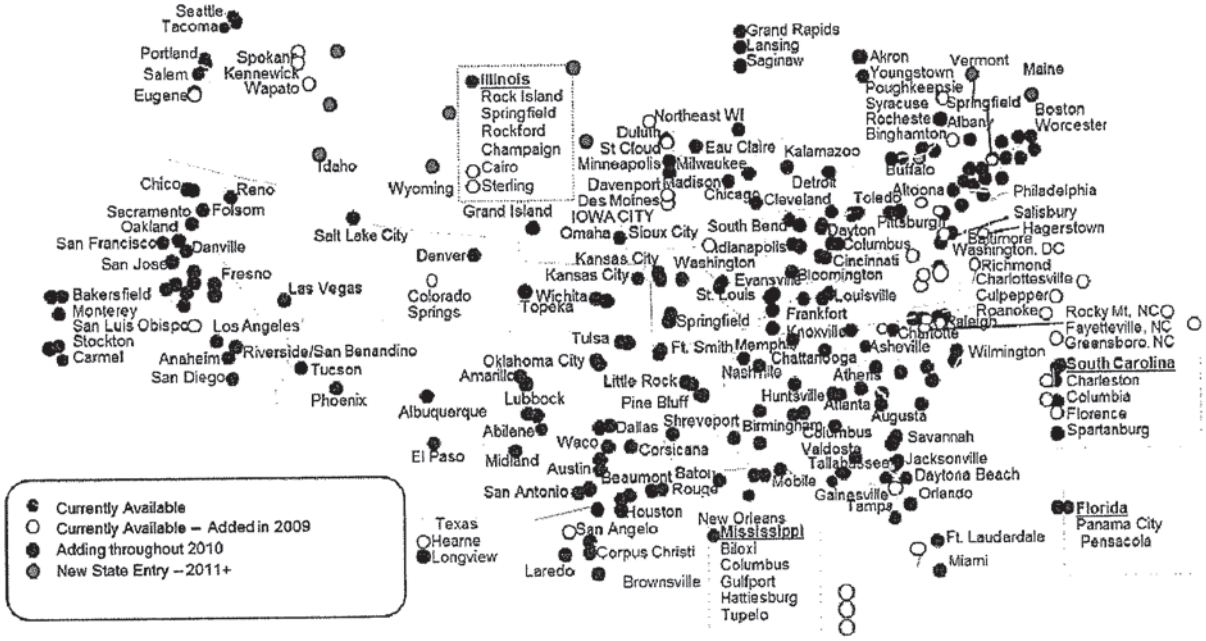
Voice DNA on Managed IP Access is available in the Domestic US (48 mainland states) within the BVoIP service area. Voice DNA on AVPN is not available with BIB. The following transports are supported:

- Access Types
  - T1
  - N x T1
  - Ethernet
- Port Types
  - PPP
  - MLPPP
  - Ethernet

Voice DNA CPE Options

AT&T can be your single point of contact for purchasing or leasing CPE solution components. These components and pricing can be found in Tab III Compensation and Cost Data.

Voice DNA Service Availability



Voice DNA is available for customer locations within the US Business VoIP footprint.

AT&T IP Flexible Reach / AT&T Voice DNA®Service Footprint

Technical Overview

Voice DNA leverages AT&T's VoIP Infrastructure, including the Call Control Element (CCE), the Border Element (BE) connection to the AT&T IP Backbone – an IP MPLS-based network and the related inherent security standards.

AT&T's VoIP architecture is based upon open standard protocols to facilitate a multi-vendor environment and to provide component interchangeability and interoperability. It is designed to support both existing and future services as they are developed and deployed.

The key elements included:

- Single IP/MPLS network with Quality of Service (QoS) and Class of Service (COS)
- Open standards architecture leveraging SIP (Session Initiation Protocol)
- A Call Control Element (CCE), which manages all signaling
- Border Elements (Bes) that "translate" the multiple protocols into SIP
- Agnostic access supporting a variety of endpoints and PSTN connectivity
- Security to preserve integrity, availability and confidentiality
- Flexibility to support emerging applications

Service Elements

The primary Voice DNA platform elements are:

- Voice DNA (Application and Media) Servers
  - Business Features (e.g., call-hold, call-pickup, call-park, call-waiting, call-forward, billing)
  - Carrier Services (e.g., Local Number Portability, routing)
  - Call Distribution features (e.g., call classification/clearing/mapping, call origin display, call prioritization/queuing, music-on-queue, automatic overflow)
  - IP Conferencing with up to 10 participants (impromptu)
- Voicemail Server

Call Flow

Call Flow in a Voice DNA environment (Inbound Flow):

1. A call enters the Public Service Telephone Network (PSTN) and goes to the nearest Network Gateway Border Element

2. The gateway converts the call into packetized IP format and queries the CCE for further instruction.

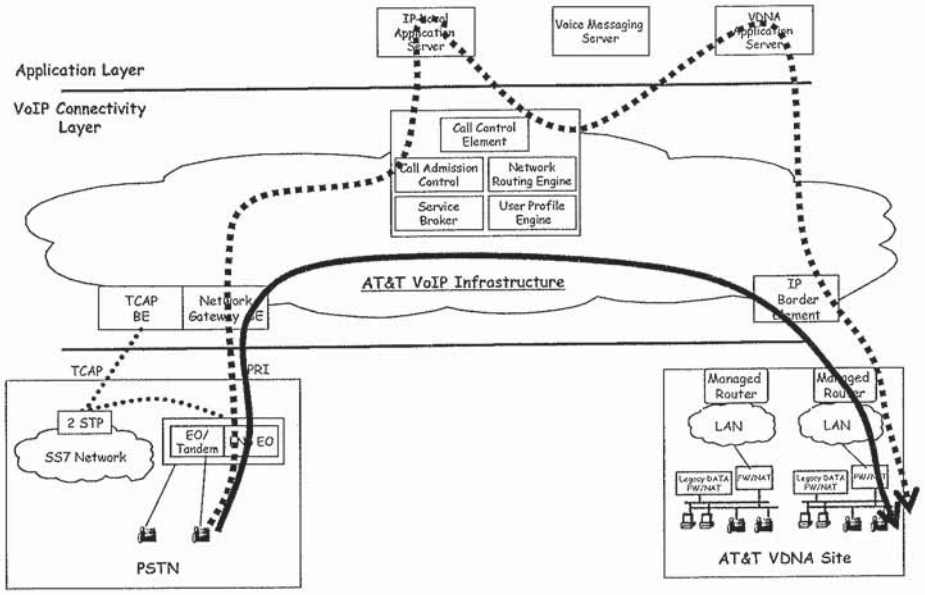
3. The CCE invokes other VoIP elements, as needed to determine the proper handling for the call. For example, the IP Flexible Reach Application Server (AS) tells the CCE that this is a Voice DNA customer and that the Voice DNA AS must be invoked. The Voice DNA AS determines if any features are active and applies these features in determining destination (e.g., call forwarding, do not disturb). With the information provided, the CCE directs the call to the appropriate IPBE/router.

4. The router determines the destination of the call and sends the packets to the appropriate station. The Voice DNA Voicemail server, in the AT&T Network, handles voicemail.

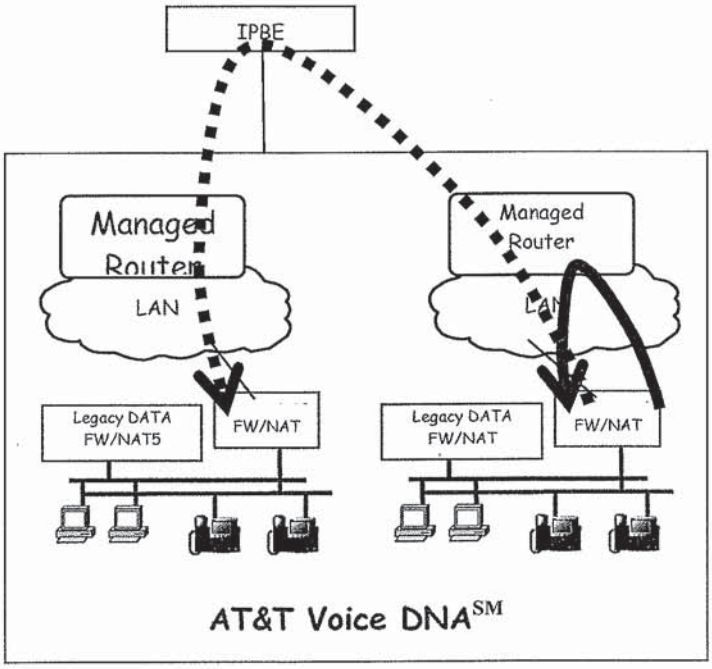
5. The call is then received at the desktop (station) IP phone.

6. Outbound calls from IP Phones follow the reverse flow – media and signaling for the inter-site and off-net calls goes up through the customer access to the IPBE; for intra-site calls, only the signal goes into the AT&T network whereas the media stays on-site.

AT&T Voice DNA Call Flow



AT&T Voice DNA℠ Call Flow – Intra-site

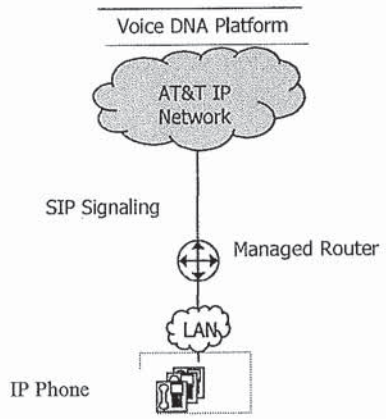


AT&T Voice DNA Application Server

The Voice DNA Application Server (AS) serves as the virtual, hosted IP PBX, providing line-side features on top of carrier-class local services and features. All Voice DNA originated calls access the Voice DNA AS for determination of customer calling features, etc. The Voice DNA AS will provide the following capabilities:

- Support multiple features (e.g., call waiting, Locate Me, conferencing, call forwarding)
- Support add-on 'a la carte" features
- Administrator Tool, including service level reports
- Personal Web Site
- Support VoIP administered private dialing plans by completing internal calls within the "Voice DNA Application" and routing all other calls to the VoIP Network Infrastructure
- IP Phone Registration
- Operations, Administrative & Maintenance capabilities

Physical Architecture



Voice DNA on Managed IP Access provides the customer with a Managed Customer Premises router. This Customer Premises router performs the necessary class of service markings and queuing capability compliant to the Converged Class of Service Project. In the Voice DNA offer the CE connects directly to the LAN that hosts the IP Phones.

Voice DNA supports AT&T managed routers. These are configured to support the AT&T Managed Integrated Device (MID) or EdgeMarc. AT&T will assign two public IP addresses. One IP address is to be provisioned on the CE router LAN interface, the second is to be provisioned on the MID WAN interface. The MID will perform DHCP and NAT functions on the customer's network and will also function as a full, stateful, customer managed firewall. This functionality positions the MID as the Voice DNA service demarcation point.

CODEC Support

All Voice DNA phones, with the exception of the Polycom 4000, use G.729 as the default voice CODEC. While G.729 offers many benefits (reduced bandwidth requirements as the single greatest benefit), it does pose voice quality concerns, especially in noisy environments and when conferencing is invoked.

Voice DNA supports the following CODECs depending on call type and device per the table below:

- G.711 – utilizes 85 Kbps of bandwidth
- G.729 – utilizes 15 Kbps of bandwidth

Customer administrators can specify on a per device basis from the Administrator Portal:

- G.711 as the preferred voice CODEC
- G.711 as the only Voice CODEC

Appendix A – Feature Descriptions

Standard Feature Package – Includes the following features and the Administrator Tool Only

Audible Call Forward

When users set their Call Forward feature ON, their phone produces a two-second stutter tone and displays a call forward message whenever an incoming call is forwarded.

- A call to a user enabled with Audible Call Forwarding and call forwarding ON, cannot be answered (e.g., upon receiving the splash tone, the user cannot answer the call even if they pick up quickly)
- Calls routed using Locate Me do not result in Audible Call Forward
- A user with Do Not Disturb turned ON will not hear Audible Call Forward tone